

EXHIBIT 31

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

DONNA CURLING, ET AL.,

Plaintiffs,

CIVIL ACTION FILE

NO. 1:17-CV-2989-AT

vs.

BRAD RAFFENSPERGER, ET AL.,

Defendants.

VIDEO-RECORDED 30(b)(6) DEPOSITION
TAKEN VIA VIDEOCONFERENCE OF
GEORGIA SECRETARY OF STATES' OFFICE
BY: SANFORD MERRITT BEAVER

AND

SANFORD MERRITT BEAVER
IN HIS PERSONAL CAPACITY
(Taken by Plaintiffs)

Atlanta, Georgia

Wednesday, February 2, 2022

9:08 a.m.

Reported stenographically by
V. Dario Stanziola, CCR (GA)(NJ), RPR, CRR

1	Exhibit 24: E-mail string with the	214
2	top from Merritt Beaver dated	
3	11/12/2020	
4	Exhibit 25: E-mail from Jason	220
5	Matthews dated 11/3/2020	
6		
7	Exhibit 26: E-mail string with the	224
8	top from Kevin Robertson dated	
9	8/14/2020	
10	Exhibit 27: E-mail string with the	226
11	top from Merritt Beaver dated	
12	3/3/2019	
13		
14	Exhibit 28: E-mail from Nick Salsman	240
15	dated 8/14/2020	
16	Exhibit 29: Document entitled	250
17	Election Office Notes: 10 am	
18	6/15/2020 Meeting	
19		
20		
21		
22		
23		
24		
25		

1 THE STENOGRAPHER: I can't hear him.

2 A. Can you hear me?

3 Q. You kind of cut in and out I think with
4 the microphone.

5 A. I can sit closer.

6 Is that -- is that better?

7 Q. Little bit. It tends to lose the first
8 word or two is what I hear.

9 A. I'm not sure what -- what to do for
10 you.

11 THE VIDEOGRAPHER: I can walk him
12 through making a quick adjustment, counsel,
13 that it should help. Would you like to --
14 it could -- it's pretty quick. We can do
15 it on the record or go ahead and go off
16 real fast.

17 MR. CROSS: We can go off.

18 THE VIDEOGRAPHER: The time is 9:10.
19 We're off the record.

20 (A DISCUSSION WAS HELD OFF THE RECORD.)

21 THE VIDEOGRAPHER: The time is 9:11.
22 We're back on the record.

23 BY MR. CROSS:

24 Q. Good morning, Mr. Beaver.

25 A. Good morning.

1 You can flip through it.

2 A. This looks -- yeah, this looks like the
3 document that counsel had shown me before.

4 Q. Okay. So scroll down to -- oh, there
5 are no page numbers. The -- sorry about that.
6 The page that has amended topics on the top. It
7 looks like it's page 7 of the PDF.

8 A. I'm there.

9 Q. And do you see topic 1 reads,
10 Implementation and operation of Georgia's current
11 election system limited to the following
12 subtopics and then there's subtopic A; do you see
13 that?

14 A. Yes.

15 Q. And then subtopic B and C are at the
16 top of the next page.

17 Do you see that?

18 A. Yes.

19 Q. And do you understand you've been
20 designated by the Secretary's office to testify
21 today on topics 1 A, B and C?

22 A. Yes.

23 Q. Okay. And then scroll down to topic 10,
24 if you would, please, which is on page 14 of the
25 PDF.

1 A. I see. Yes.

2 Q. And do you understand you've been
3 designated to testify on that topic today?

4 A. Yes.

5 Q. And then if you come to the last topic,
6 18, on page 15; do you see that?

7 A. Yes.

8 Q. And do you understand you've been
9 designated to testify on that topic today as
10 well?

11 A. Yes.

12 Q. Are there any other topics in here that
13 you understand you're designated to testify on
14 today that we've not addressed?

15 A. Give me a moment. No.

16 Q. Okay. All right. Come back to topic
17 1A, if you would, please.

18 A. 1A. I'm here.

19 Q. And what did you do to prepare to
20 testify on topic 1A today?

21 A. I went and validated -- first off,
22 let's define malware. Malware is an application
23 program that runs on a computer that was
24 basically designed to do an action of some sort,
25 all right?

1 to do anything with the old system. When we
2 finished using the old system we just turned it
3 off.

4 Q. When did that happen?

5 A. We walked away from it.

6 Q. When did that happen?

7 When did you turn off the old system?

8 A. It was -- I'd have to go back and look.
9 I mean, I'd be guessing right now.

10 Q. Do you have any time frame?

11 Was it 2019 when you rolled out the new
12 system or was it 2020?

13 A. We had the old system still on -- I'll
14 say turned on. But we essentially -- we call it
15 put it over in the corner because nobody was
16 using it for about six months just in case there
17 was any questions about something that was done
18 in that system. So it would be somewhere towards
19 the end of '19, probably into early 2000 that we
20 literally unplugged it.

21 Q. And did servers from the old system sit
22 in the same environment as the new system at any
23 point?

24 A. Nope. They were in totally different
25 racks. In fact, the rack was on wheels. When we

1 finished we literally rolled it into a caged area
2 that was locked, pulled all the cables off of it
3 and left it in a secure area. So it -- nobody
4 could accidentally get into it. It would have
5 taken somebody from my group to go reset it up.

6 Q. Okay. Who did you meet with you said
7 about two or three weeks ago to validate this for
8 the system?

9 A. Who did I meet with? My director of
10 technology. My -- a couple of the people that
11 work with him.

12 Q. What's his name?

13 A. Jason Matthews.

14 Q. You said Jason Matthews?

15 A. Yeah, Jason Matthews.

16 Q. And who else did you meet with?

17 What are their names?

18 A. Ronnell Spearman and Kevin Fitts.

19 Q. And they are report to the director of
20 technology?

21 A. Yes.

22 Q. And were they the ones that were
23 responsible for setting up the -- the new system
24 and turning off the old one?

25 A. Ronnell was involved in that group,

1 Jason was involved in that group. I think Kevin
2 was more on the sidelines, was being informed as
3 to what was going on. He was part of the team
4 that -- that was more consulted as to what we
5 should do. But I don't know that he had any
6 hands-on.

7 Q. Do they have log-in credentials for the
8 Dominion EMS server at the state?

9 A. Yes.

10 Q. Do you?

11 A. No.

12 Q. Who else has log-in credentials for the
13 state Dominion EMS server?

14 A. On the -- it's called the
15 infrastructure team. Those are the IT people
16 that manage the servers. They're probably maybe
17 two, two other people.

18 Q. And they're on the infrastructure team?

19 A. Yes.

20 Q. Okay. Do you know if anyone in Michael
21 Barnes's office has log-in credentials?

22 A. I have one person that's on the
23 infrastructure team that works over in his group.
24 And I believe he does. His group is actually in
25 a different building. So we -- we have to have

1 somebody on site to support his group.

2 Q. You said there's no equipment used with
3 the old system that's used with the new system.
4 Did I understand that right?

5 A. Correct. The old system was
6 Windows-based running access. It's a very old
7 Windows 2000 environment. The new system is
8 Android-based.

9 Q. The -- the individuals who have log-in
10 credentials for the new system for the EMS
11 server, did you guys replace all of their laptop
12 computers, any electronic equipment that they use
13 for their work with respect to elections?

14 A. Are you saying the -- the people that
15 work over in the -- in election center? The
16 people that use this new environment?

17 Q. I'm saying anyone who has access or
18 uses this new environment, did you replace all of
19 their electronic equipment that they use for
20 their work? So computers, laptops, removable
21 media?

22 A. Yes, all -- all desktops, everything
23 connected to that new environment, including the
24 wires in the wall, were all brand new. The
25 desktop computers that they used to tie into it

1 were brand new. We started clean, fresh. We did
2 not take any chances by introducing anything old.

3 Q. And how do you -- I'm sorry. Go ahead.

4 A. We did not share any of the networking
5 infrastructure. That was all new.

6 Q. And are you saying -- you're also
7 saying that there is no data in the old system
8 that's used with the new system?

9 A. Correct. As I said, it's not
10 compatible.

11 Q. So how does that work for the data in
12 E-Net? Doesn't --

13 A. So -- so for the new system, we had to
14 go back to E-Net and get new data and bring it
15 over to the new system.

16 Q. All right. So how did you do that?

17 I thought you said there's no data from
18 the old system used in the new system?

19 A. The old system -- there are multiple
20 systems. Their E-Net is not the voter -- the
21 votering balloting system. The question that
22 this test talks about is all of the ballot and
23 voting system, not the voter registration system.
24 So when you're speaking of the system, I need you
25 to tell me which system you're talking about. So

1 voter registration system is different than the
2 ballot generation system that feeds the -- the
3 vote-taking system, the voting system. It's two
4 complete environments. Two totally different
5 systems.

6 Q. So you don't --

7 A. The only thing that comes from one to
8 the other is E-Net will export information about
9 candidates over to the balloting system.

10 Q. Do you not consider Georgia's voter
11 registration system part of the state's election
12 system?

13 A. That is an umbrella statement. And
14 when you say the election system, there are
15 numerous systems. They're not tied together.
16 They're all independent systems that are run and
17 managed independently. So you can't apply
18 something about one system to the other system.
19 Operating systems are different, applications are
20 different. The actual users are different.

21 Q. So let me -- let me just make sure I
22 understand. I just want to see -- so does
23 Georgia's election system include the voter
24 registration database or that's something
25 separate?

1 included in the election system today?

2 A. So they -- at the data center where the
3 election system is held there is a whole network
4 environments which components for security and
5 basically segmenting networks, the actual
6 environment itself. Each of our environments
7 have those kind of components in it. They're not
8 necessarily the same. They're different based on
9 the system that it's protecting and the system
10 it's supporting.

11 Q. Anything else, any other components?

12 A. I'm sure there's other more detailed --
13 I mean, depending on how granular we want to get
14 into defining what an environment is holding.
15 But those are the high level things.

16 Q. Okay. What interactions are there, if
17 any, between the Dominion air gaps election
18 system that you talked about earlier that you
19 said is air gapped and the voter registration
20 database or E-Net?

21 A. Well, there is not necessarily
22 interaction between the two. There is a data
23 transfer that happens for each election where
24 somebody from the election center will download a
25 file from E-Net, it will go through numerous

1 security checks and then it gets uploaded into
2 the air gap environment following NIST protocols,
3 that's the National Institutes of Science and
4 Technology. They're the ones that define that we
5 follow defining an air gapped environment.

6 Q. And you said that -- so the data gets
7 transferred from E-Net into the Dominion EMS for
8 a particular election and it goes -- that process
9 goes through numerous security steps.

10 What are those security steps?

11 A. So the device that gets used gets
12 formatted by an independent device that's not
13 tied to a computer. It's strictly a formatter.
14 It's literally a hardware device that you plug
15 electricity into the wall. That's it. It has no
16 operating system other than a hard program that's
17 formats a USB. So nothing could ever get stored
18 on it. It formats the USB drive to clean it so
19 that we know nothing has ever moved to it or
20 anything that was on it is off.

21 Then it gets inserted into a PC that's
22 tied into the election system. It is immediately
23 scanned -- once the file comes down to that thing
24 it's immediately scanned for any malware, any
25 strange things that could be also on it. Then it

1 gets moved over to the -- a PC that's tied into
2 the air gapped environment and it gets uploaded.

3 Q. And is that device, is that a hard
4 drive?

5 A. It's a flash drive.

6 Q. Oh, okay. And is that a new flash
7 drive every time these transfers are done or are
8 those flash drives reused?

9 A. Potentially could be reused. But as I
10 said, they get completely formatted by a box that
11 is not tied to any Internet. Cannot have
12 anything stored on it. So if there was anything
13 on that flash drive, doesn't matter what it was,
14 it can't transfer off to the formatter. The
15 formatter will format that completely blank.

16 So anything on it, malware, anything is
17 erased. There's no transferring of old data to
18 the formatter because the formatter is not
19 intelligent to be actually able to hold anything.
20 It just has a function of format. So it is
21 probably cleaner than a brand new purchased -- in
22 fact, I'll tell you it is cleaner than a brand
23 new purchased flash drive. Even if we use a
24 brand new purchased flash drive, we clean it
25 first just in case the manufacturer had something

1 on that drive that they didn't know about, we
2 don't trust it. We clean it.

3 Q. Are ballot definition files stored on
4 the state EMS for each election?

5 A. On the state EMS? What do you mean?

6 Q. The state EMS server, are ballot
7 definition files uploaded to that server each
8 year or for each election?

9 MR. DENTON: Objection.

10 A. I don't know the term EMS.

11 Q. Election management system, the
12 Dominion -- the state server that we're talking
13 about.

14 A. Oh, the ballot building system.

15 Q. Yes. Yes. They're -- let's just back
16 up, make sure we're talking about the same thing.
17 What we've been talking about is a server that
18 the state uses that has the Dominion software on
19 it to run elections, right?

20 A. Yes, that's the ballot building system.

21 Q. Okay.

22 A. So when you say EMS, now I understand
23 what you're saying.

24 Q. Right.

25 And have you heard the term election

1 the process. You can't use any of the old system
2 information in the new environment.

3 Q. But you don't know, for example,
4 whether the counties use some of the same USB
5 drives, flash drives that they plugged in or used
6 with the old system, you don't know whether some
7 of them used those with the new system, right?

8 A. As I said, it's incompatible. The
9 flash drives were not the same as the current USB
10 drives. They weren't USB. They were a different
11 format. The plug on them wouldn't fit.

12 Q. You're saying that it's your belief
13 that the USB drives the counties use with the
14 with respect to elections on the GEMS system, the
15 DRE system, those wouldn't even plug into
16 equipment that they used with the BMD system; is
17 that -- is that really your belief?

18 A. The DREs, this is the Windows-based
19 voting equipment, had a different format for
20 their flash drive. They were a square drive
21 device that had, I don't know, 40-hole --
22 pinholes in it. Wouldn't even come close to
23 fitting in a USB drive, which has got a very
24 rectangular slide-in port. So the DREs took a
25 different format flash drive.

1 Q. But the DREs are not the only part of
2 the election system at the county level that uses
3 flash drives, right?

4 They also use desktop computers, laptop
5 computers, they have their own election servers
6 such as for election night reporting, for
7 managing their own system. And those would take
8 the same flash drives that would fit on equipment
9 today, right?

10 A. You asked me about a DRE interface. I
11 answered you about a DRE interface. So now then,
12 now you're asking me whether or not they have
13 computers that use USB flash drives, which is
14 yes. The new system has computers which can
15 accept USB drives, yes.

16 Q. And you've not undertaken any
17 investigation to determine whether the counties
18 got rid of all their old flash drives and
19 replaced them with new flash drives when the new
20 Dominion system was rolled out; is that fair?

21 A. So if you're asking me if a USB drive
22 that was used with the old DRE system that was
23 running a Windows application using an access
24 database program that potentially could have had
25 malware that was attacking that system, which

1 built it out, as I said, as a clean system. We
2 did not use anything that was tied to the
3 Internet where malware can come into it, get in,
4 infect it. We have only entered the information
5 that has been scanned for malware into that
6 environment.

7 Q. So no one, to your knowledge, has
8 actually gone in and done any kind of forensic
9 analysis of any of the BMDs or the Dominion
10 servers at the state or county level to see if
11 they are infected with malware; is that right?

12 A. I'm not aware of that.

13 Q. Do you know why that has not been done
14 even on a sampling basis, for example?

15 A. Not aware that there's any sign that
16 there is any malware on it. That's usually the
17 first trigger to look for malware. That would be
18 it.

19 Q. Well, you understand malware can
20 successfully operate in the background without
21 giving an indication that it's there, right?

22 MR. DENTON: Objection.

23 A. Yes, I do. But then I follow back to
24 the tenet we talked earlier is that malware has
25 to somehow physically get onto that environment

1 and have programming logic that is compatible
2 with the environment that it's in.

3 Q. Right.

4 And I understand that, Mr. Beaver.

5 A. Okay.

6 Q. But -- okay. I get it. Thank you.

7 All right. Take a look at topic 1 B,
8 please. Just let me know when you're there.

9 A. Yes. Yes, I'm there.

10 Q. This is any efforts made to air gap a
11 components of Georgia's current election system
12 and the success or failure of any such efforts.

13 A. The answer -- the answer is yes.

14 Q. Right.

15 And so what are those efforts?

16 A. So Secretary of State's IT group,
17 department built an air gapped environment based
18 on NIST standards using NIST protocols to hold
19 the Dominion ballot building environment. And
20 continues to maintain that air gapped environment
21 per the NIST protocols.

22 Q. And that was built sometime in 20- --

23 A. '19.

24 Q. Oh, 2019?

25 A. I think it was -- yes.

1 Q. All right. And this was what you were
2 talking about earlier that it's all new
3 equipment, even new wires in the wall?

4 A. Yes.

5 Q. Okay.

6 A. It does not share anything with any
7 other network environment. It does not
8 cohabitate in any racks or environment.

9 Q. Right.

10 But it does share data with the voter
11 registration system, though, right?

12 A. Yes. And that data is transferred
13 using the NIST protocol.

14 Q. Okay. Who at the Secretary's office is
15 actually responsible for transferring that data?

16 A. That would be Michael Barnes's group.

17 Q. Okay. Who is responsible for uploading
18 any data or files to the state EMS server for any
19 given election?

20 Is there anyone on your team that does
21 that or is that also Mr. Barnes's group?

22 A. That's Mr. Barnes.

23 Q. Okay. All right. Take a look at topic
24 1 C, please.

25 A. Okay.

1 component?

2 A. Oh, hold on.

3 Q. It's for the --

4 A. Component list limited to the following
5 equipment for election...

6 So this all looks like it's speaking to
7 the current Dominion environment, meaning the
8 ballot building device --

9 Q. Yes.

10 A. -- environment.

11 Q. Yes, that's right.

12 A. It doesn't speak to any of the voter
13 registration system, the my voter page, the
14 online registration page. It's just the Dominion
15 environment.

16 Q. Correct. Yeah.

17 A. Okay.

18 Q. And so let's --

19 A. So now --

20 Q. Yeah, let's start with that. So take a
21 look at -- with that definition in mind, are you
22 aware of any connections to the Internet,
23 telephone lines, cable lines, satellites or other
24 third-party system or network for any of the
25 components identified in footnote two for the

1 current election system?

2 A. None.

3 Q. And what's the basis for that belief?

4 A. We have built an air gapped
5 environment, follows, as I've said, the NIST
6 protocols on its own dedicated hardware network
7 environment. Does not share anything with an
8 environment that has any of these types of
9 things, Internet, telephone, cable, satellites or
10 other third-party networks, is not tied to
11 anything that would have those things connected
12 to it.

13 Q. Okay. But you don't know, for example,
14 whether any of the 159 counties have ever
15 connected any of those components to any Internet
16 or third-party system, right?

17 MR. DENTON: Objection.

18 A. We're talking about what was described
19 above and that everything that's described above
20 is that Dominion environment, which is based in
21 our election center in Marietta. So the counties
22 don't have access to that.

23 Q. Well, no. Look -- if you look at
24 footnote two it includes the Dominion BMDs, the
25 printers used with the Dominion BMDs, the

1 scanners used to scan ballots, servings --
2 servers containing election management system --

3 A. So you're talking about the actual
4 equipment that's in the field?

5 Q. Correct. That's part of it. Yeah.

6 And so you don't -- so you don't know
7 as you sit here whether any of the 159 counties
8 in Georgia has ever connected any of that
9 equipment to the Internet or to a third-party
10 system, right?

11 A. No. I mean, there's some of the stuff
12 that can't be connected, like the BMDs don't have
13 a network connection to go into that. Now, a
14 laptop, I'm not sure what a laptop -- what they
15 would use a laptop for, a desktop computer, not
16 sure how that would be involved in this whole
17 environment. So I can't speak to those things.
18 Smart phones, same thing, like I -- it's -- it's
19 listed in this list, but it isn't necessarily
20 used in the Dominion environment.

21 So this is a very large list of things,
22 but not all of them have anything to do with the
23 Dominion environment. But I can't speak to, you
24 know, what the counties have done with these
25 kinds of things.

1 Q. All right. The Dominion BMDs used in
2 Georgia have a standard USB port on them, right?

3 A. Yes.

4 Q. In fact, the detached printer that
5 prints the ballot connects to the BMDs with
6 standard USB port, right?

7 A. Yes.

8 Q. And are you aware that the Dominion BMD
9 USB ports are not sealed, meaning that a voter,
10 for example, has access to plug in a USB drive to
11 a BMD used in an election?

12 A. I don't believe that's true. It was a
13 term it's sealed. It's not sealed. I have never
14 seen an environment where it's not sealed. So
15 I'm not sure where that comes from. So I guess I
16 can't answer that that would be true. I am not
17 aware that that -- that system is not sealed.

18 Q. So what is the basis for your
19 understanding that the USB port on each of the
20 30,000 BMDs in Georgia is sealed?

21 A. I've seen them and they're sealed. And
22 that is our protocol is to keep it sealed.

23 Q. Well, I assume you haven't seen all
24 30,000 BMDs, right?

25 A. No, I -- yeah, I haven't seen 30,000

1 BMDs. But, as I said, the protocol is to keep
2 them sealed. And when I say sealed, they're
3 locked -- locked away. They have a sealing
4 device that will show tampering if somebody
5 unseals it. So I have not heard of any counties
6 that have had an issue with BMDs being unsealed.
7 I have not heard that.

8 Q. Okay. And is that something you would
9 expect to know as the state CIO?

10 A. I would have heard it. It isn't the
11 counties report to me. You could probably ask
12 Mr. Michael Barnes if he's heard it. I think
13 he's more in touch with the counties than I am.

14 Q. And why is sealing the BMDs important?

15 A. Many type of layers of security.
16 Security is not just one thing. It is a layer
17 approach. Sealing the BMD is just one of the
18 many security aspects to that -- verifying that
19 we have a very secure system. Sealing is a piece
20 of it.

21 Q. But what is the sealing of a BMD
22 intended to protect against?

23 A. Just what you described, somebody
24 having access to do something to it that's
25 unknown.

1 Q. Got it.

2 Okay. And would it be fair to say that
3 if -- that if -- if a county found that its BMDs
4 were unsealed, the seals were broken, for
5 example, before an election, they should not use
6 those, right?

7 A. Correct. That is the protocol.

8 Q. Okay. What's the device that's used to
9 seal the USB ports on the BMDs?

10 A. I don't know what that device is.

11 Q. All right. Jump to topic ten, please.

12 A. Okay.

13 Q. Topic ten is any instance in 2020 or
14 2021 within the knowledge of the Secretary of
15 State's office when a person or entity other than
16 an authorized election worker of Georgia state or
17 county official obtained voting data from a
18 Georgia election or images of voting equipment
19 used in a Georgia election.

20 Do you see that?

21 A. Yes.

22 Q. And are you aware of any such instance?

23 A. I am not aware of any instance.

24 Q. And would you expect to be aware of
25 this as the state CIO if -- if this was known to

1 does have the authority to require cybersecurity
2 assessments of its vendors, right?

3 MR. DENTON: Objection.

4 A. I don't know. That's a good question.

5 Q. You're not aware of a rule that
6 actually requires the Secretary of State's office
7 to ensure that vendors that are related to the
8 election system do cybersecurity assessments?

9 A. Are you saying annually?

10 Q. Annually or on any schedule. Sorry, go
11 ahead.

12 A. I am not aware of a rule or any
13 legislation or anything that says that. I think
14 that is good practice that we have built over the
15 years since I've been here. But I don't know of
16 any rule. I've never been told of any rule that
17 states that.

18 Q. Okay. The cybersecurity assessment for
19 CES that's done annually, is that -- is there a
20 written report of that?

21 A. We don't do written reports now.

22 Q. When you say now, when did that -- when
23 did that start?

24 A. The last two years.

25 Q. Why are there no written reports of ooh

1 cybersecurity assessments for the Secretary's
2 office as of the last two years?

3 MR. DENTON: Objection.

4 Q. You can answer it.

5 Do you know why?

6 A. Yes. They're taken out of context by
7 the public.

8 Q. What do you mean?

9 A. They read them, they don't understand
10 them, they take them out of context.

11 Q. So how is the cybersecurity assessment
12 the -- the steps that are taken and the findings
13 conveyed to folks at the Secretary's office if
14 not in writing?

15 A. We have conference calls. I have a
16 working team that works with Fortalice. We
17 review things that they say you need to be
18 looking at this, you need to be looking at that.
19 We look at our project lists of tasks that we
20 need to do across the board to figure out how do
21 we mold some of those in. Or not some of those,
22 but mold those things in. Made our life
23 difficult.

24 Q. You mentioned Fortalice. Is Fortalice
25 the one that does the annual cybersecurity

1

[REDACTED]

■

■

[REDACTED]

■

■

[REDACTED]

■

[REDACTED]

[REDACTED]

■

[REDACTED]

■

■

[REDACTED]

■

■

[REDACTED]

[REDACTED]

■

[REDACTED]

■

■

[REDACTED]

■

[REDACTED]

■

■

[REDACTED]

■

■

[REDACTED]

■

■

[REDACTED]

■

[REDACTED]

[REDACTED]

■

[REDACTED]

[REDACTED]

[REDACTED]

■

[REDACTED]

■

[REDACTED]

[REDACTED]

■

■

[REDACTED]

[REDACTED]

■

[REDACTED]

■

■

[REDACTED]

■

[REDACTED]

[REDACTED]

■

■

[REDACTED]

■

[REDACTED]

■

[REDACTED]

■

[REDACTED]

■

[REDACTED]

1

A.

[REDACTED]

[REDACTED] [REDACTED] [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] [REDACTED]

[REDACTED] [REDACTED]

[REDACTED] [REDACTED] [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] [REDACTED]

[REDACTED] [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] [REDACTED]

[REDACTED] [REDACTED]

[REDACTED]

[REDACTED] [REDACTED]

[REDACTED]

[REDACTED] [REDACTED]

[REDACTED] [REDACTED]

[REDACTED]

[REDACTED]

11

11

[REDACTED]

11

5

2

1

[REDACTED]

■

[REDACTED]

■

[REDACTED]

■

■

[REDACTED]

■

[REDACTED]

■

[REDACTED]

■

■

[REDACTED]

■

■

[REDACTED]

■

[REDACTED]

■

[REDACTED]

■

■

[REDACTED]

■

■

[REDACTED]

[REDACTED]

[REDACTED]

■

■

[REDACTED]

■

[REDACTED]

■

■

[REDACTED]

■

[REDACTED]

■

[REDACTED]

■

[REDACTED]

[REDACTED]

■

[REDACTED]

[REDACTED]

■

[REDACTED]

■

[REDACTED]

■

■

[REDACTED]

■

[REDACTED]

■

[REDACTED]

■

[REDACTED]

1 that also the same process today with Dominion
2 and the poll pad software that's used?

3 A. That would be a Michael Barnes
4 conversation.

5 Q. Okay. Is it your belief that logic and
6 accuracy testing done on BMDs provide
7 cybersecurity assessments for those machines?

8 A. It is one of the layers we use.
9 Remember I said that security is not one thing,
10 it's one of many layers. It's an important to
11 valid validate that the software that's on there
12 is what you expect to be on there and there's
13 nothing else on that system. So yes, it is one
14 of the layers.

15 Q. And is it your understanding that logic
16 and accuracy testing actually validates the
17 software that's on a given BMD?

18 A. It validates that it matches a hash
19 test. Means if you hash the file, you will get a
20 respondent hash. If you hash a file that has
21 been modified at all or is of a different
22 structure, meaning something hiding there with
23 the same name, it will come back a different
24 hash. And it will fail.

25 Q. But do you understand that it's common

1 with malware to design malware so that it defeats
2 the hash test, meaning it will spit back the same
3 hash that you're looking for when you're doing
4 something like logic and accuracy testing?

5 MR. DENTON: Objection.

6 A. I don't have any -- any document that
7 says that.

8 Q. That's not something you've heard
9 before?

10 A. Nope.

11 Q. Okay. All right. Take a look at
12 paragraph 18, please.

13 Do you have that in front of you?

14 A. Yes, I do.

15 Q. And here you wrote, State defendants
16 also conducted parallel testing on election day
17 for a copy of an actual county GEMS database is
18 used with a voting machine set up in the
19 Secretary of State's office and set an election
20 mode for a specific real county precinct.

21 Do you see that?

22 A. Yes.

23 Q. Is that same sort of parallel testing
24 done today with the Dominion system?

25 A. I'm not aware of that.

1 A. Yes.

2 Q. Do you have an understanding as to
3 whether the Dominion BMD system is software
4 independent?

5 A. I'm not sure I understand your
6 question. It's software independent.

7 Q. Sorry. The question is just that do
8 you have -- do you have any understanding as to
9 whether the Dominion BMD system used in Georgia,
10 whether it's considered software independent?

11 MR. DENTON: Objection.

12 A. I've never heard that term.

13 Q. Okay. Where she goes on to say that
14 the system must be auditable and its tabulation
15 record cannot be based solely on its software, do
16 you have an understanding of whether the
17 tabulation record in Georgia with the DM -- the
18 BMD system is based on the software?

19 MR. DENTON: Objection.

20 A. I can tell you there's no voting on a
21 BMD system. All you're doing is marking a
22 ballot. So if somebody says you are maliciously
23 changing votes, there are no votes counted on a
24 BMD. So I am -- you know, I can only speculate
25 here. But the whole conversation is sideways.

1 Q. Okay. All right. Thank you.

2 All right. You can put that aside.

3 Sorry. I accidentally closed Exhibit
4 Share.

5 (Exhibit 9: Document entitled
6 Information Technology Security Program
7 Charter marked for identification, as of
8 this date.)

9 Q. All right. Let me put up the next
10 exhibit. This will be Exhibit 9, Mr. Beaver.

11 MR. DENTON: David, while that's
12 loading, if you're through with Exhibit 8,
13 I don't know whether you are, but I know
14 there have been people on this deposition
15 who should not have access at this time.
16 And that I know, for example, Ms. Marks was
17 in here earlier and indicated that she had
18 access to Exhibit Share. So it might make
19 sense to pull Exhibit 8 back out of the
20 share folder for now.

21 MR. CROSS: I don't have a problem with
22 that. But I don't think I have the ability
23 to do that. Looks like maybe I could block
24 it. See what this does.

25 THE VIDEOGRAPHER: This is the

1 videographer. I'm not sure about the
2 ability to lock or unlock. But I know once
3 a exhibit is introduced into Exhibit Share,
4 the only people that could remove it is
5 Veritext. So I can e-mail them and ask
6 them to remove it if I need to.

7 Q. Mr. Beaver, see if -- and you can try
8 to, see if you can open Exhibit 8 now. I just
9 locked it. I don't know if that means you guys
10 can no longer open it.

11 A. I just opened it again.

12 Q. Oh, you did?

13 A. Yes.

14 MR. CROSS: Alex, can you open
15 Exhibit 8?

16 MR. DENTON: I can as well.

17 MR. CROSS: Oh. All right. It doesn't
18 let me pull it out. But...

19 A. Can we lock out people from joining?

20 MR. CROSS: I don't think Ms. Marks is
21 coming back. But if she comes on, we can
22 -- we can deal with that.

23 MR. DENTON: Yeah, my -- I don't have a
24 full understanding how of how Exhibit Share
25 works. I think you can probably

1 independently access it at any point
2 whether you -- regardless of whether you're
3 in Zoom. So to the extent --

4 THE VIDEOGRAPHER: That is correct.

5 MR. DENTON: To the extent that that's
6 something that needs to be -- have limited
7 disclosure right now, it sounds like from
8 Mr. Miller that we may -- Jonathan Miller
9 that we may need to ask Veritext to pull
10 that back.

11 MR. CROSS: Okay. All right.

12 THE VIDEOGRAPHER: Would you all like
13 me to ask them to do so, counsel?

14 MR. CROSS: Yeah, why don't you, if you
15 don't mind, ask them to pull Exhibit 8 out.

16 THE VIDEOGRAPHER. Exhibit 8. Got it.
17 I'll take care of it. Thank you, sir.

18 MR. CROSS: All right. Thank you.

19 BY MR. CROSS:

20 Q. All right. Mr. Beaver, do you have
21 Exhibit 9 in front of you?

22 A. Yes, I do.

23 Q. All right. Have you seen Exhibit 9
24 before?

25 A. Is there a date on it? Oh, let's see.

1

2

3

4

Q. Okay.

5

A. But I don't recall it specifically.

6

7

Q. Okay. All right. I'll give you the next exhibit.

8

9

10

11

12

13

MR. DENTON: And David, I guess a similar comment as to Exhibit 9, this looks like a forward produced document under the confidential AEO designation. So it probably requires the same treatment as Exhibit 8.

14

15

16

17

18

MR. CROSS: So let's do this, what we've done in the past is -- I don't want to start pulling exhibits out. It's going to get really confusing. Jonathan, can you just -- are you still there?

19

20

21

22

23

24

25

THE VIDEOGRAPHER: Yes, sir.

MR. CROSS: Can you just ask Veritext to remove Marilyn Marks' access to this exhibit folder if she has it. That's what we've done in the past. So she will not --

THE VIDEOGRAPHER: I will ask if they can do that. They may or may not be able

1 to do that. I'm not hundred percent sure.
2 But I will ask.

3 MR. CROSS: Okay. I know they've done
4 it in the past when we've had a situation
5 --

6 THE VIDEOGRAPHER: And she specifically
7 needs to not have access to Exhibit 8 only?

8 MR. CROSS: No, just pull that access
9 to Merritt Beaver entirely. Because there
10 are going to be a number of confidential or
11 AEO documents.

12 THE VIDEOGRAPHER: Pull her access to
13 the folder for today entirely, correct?

14 MR. CROSS: That's correct.

15 THE VIDEOGRAPHER: Okay. That's easy
16 to do. I can -- I can take care of that.

17 MR. CROSS: All right. Thank you.

18 (Exhibit 10: Document entitled
19 Fortalice Solutions Web Vulnerability
20 Remediation Checks Secretary of State
21 Georgia Draft - July 14, 2020 marked for
22 identification, as of this date.)

23 BY MR. CROSS:

24 Q. Okay. All right. Grab Exhibit 10,
25 please, Mr. Beaver.

1 file, somebody's taken over my computer when in
2 reality it was a pilot error. So this was
3 classified as an event, not an incident.

4 Q. Okay. And what's the distinction you
5 draw between event and incident?

6 A. So an event is when something has
7 flagged as a suspicious activity or something
8 that looks wrong that deserves somebody to do
9 investigation. Once you identify, you know, that
10 there is malicious activity going on, it gets
11 transferred to status of an incident and you
12 start a process called an incident response
13 process, which is bringing in the -- you know,
14 the appropriate people, starting to document it,
15 things like that.

16 Q. Okay. And do I understand correctly
17 that there's no written report on Fortalice's
18 findings because of the policy for them not to
19 generate reports on this?

20 MR. DENTON: Objection.

21 A. I don't recall -- I don't recall. Even
22 a -- like a document. I just remember hearing
23 oh, it's -- there's nothing there. They've
24 searched it.

25 (Exhibit 13: E-mail string with the top

1 A. Yeah.

2 Q. And he writes, I am the IT director for
3 the Georgia Secretary of State.

4 Do you see that?

5 A. Yes.

6 Q. Are you familiar with them?

7 A. With Clark Rainer?

8 Q. Yes.

9 A. Yes. He used to work for me.

10 Q. Okay. And is he gone now too?

11 A. Yes. He's the CIO for the -- I think
12 it's the AG office.

13 Q. The Georgia Attorney General's office?

14 A. Yes.

15 Q. When did he move into that role,
16 approximately.

17 A. It was I think early 2020.

18 Q. Okay. If you come down --

19 A. It was after Raffensperger came over.
20 It was soon after Raffensperger came over.

21 Q. Okay. If you come down to the bottom
22 of the first page, do you see he's got four
23 bullets?

24 A. Yes.

25 Q. And the last bullet on that page,

1 number 4 reads, Just got an e-mail from MS-ISAC
2 with some more information I'll forward on in
3 just a minute. Also showing you may have a
4 malware infection.

5 Do you see that?

6 A. Yes.

7 Q. And this is being sent to Josh Hood,
8 professional services technician.

9 Do you see that?

10 A. Yes.

11 Q. Who is Josh Hood?

12 Do you know who that is?

13 A. No, I don't.

14 Q. Okay. What do you know, if anything,
15 about this situation in the -- what Mr. Clark or
16 what Mr. Rainer wrote about a possible malware
17 infection?

18 A. Nothing. We get -- we get reports from
19 counties I'll say on a regular basis about
20 different malware attacks where a county office
21 will -- somebody will have clicked on something
22 and they realize that something happened to their
23 network and they'll send out a message to
24 everyone saying hey, you know, we're in the
25 process of cleaning our systems because of X, Y

1 and Z. This looks like this might be a very
2 similar thing where they were reaching out to us
3 for some help.

4 Q. Okay.

5 A. But I don't have any specific recall of
6 this event.

7 Q. And you don't recall whether there was
8 any investigation or any findings?

9 A. No. As I said, it is not an unusual
10 conversation to go with the counties when they
11 have an event where somebody clicks on something
12 that they'll notify us just to make sure that,
13 you know, we know what's going on so that if --
14 if for some reason we start getting e-mails from
15 them that look weird or something like that, we
16 know like, oh, they've got something that's
17 happened in their environment, let's be careful.

18 So, I mean, Clark was just trying to be
19 helpful in that, you know, we reached out to --
20 we have a tie -- most of the counties have a tie
21 into MS-ISAC also. I'm sure he had reached out
22 to MS-ISAC with this information and may have
23 gotten information that -- back from them. I
24 mean, they cover election systems across the
25 country. One of the reasons we work with them is

1 because we get to see a -- a national view of
2 attacks. And so if one state is getting attacked
3 -- has an attack going on or something happens,
4 we can get that information and helps us protect
5 ourselves against similar attacks. So Clark is
6 just trying to help him understand, you know,
7 that MS-ISAC may have a bigger view into what's
8 going on.

9 (Exhibit 15: E-mail string with the top
10 from Dave Hamilton dated 8/13/2020 marked
11 for identification, as of this date.)

12 Q. Okay. So grab Exhibit 15, if you
13 would, please.

14 A. Dave Hamilton potential leak -- leakage
15 of voter data.

16 Q. Yes.

17 So this is an e-mail that Dave Hamilton
18 sent on August 13, 2020, right?

19 Do you see that?

20 A. Okay.

21 Q. And if you come down to the earliest
22 e-mail on the thread at the bottom, it's an
23 e-mail from -- the name is K-I-J-Y-U-U, and the
24 last name it looks like is Tradebit,
25 T-R-A-D-E-B-I-T, August 12, 2020.

1 Do you see that?

2 A. Are you on the last page?

3 Q. I'm at the top of the last page, bottom
4 of the second to last page.

5 A. Oh, yeah, yeah, yeah, yeah, Tradebit,
6 Tradebit.

7 Q. And so if you come to the -- the e-mail
8 this person sends indicates in the first
9 sentence, I would like to say someone anonymous,
10 but I am contacting you because I have worked
11 with you in the past a little and I knew you
12 would be a good person to contact.

13 Do you see that?

14 A. Yep.

15 Q. And then he goes on in the next
16 paragraph to indicate that he's discovered a flaw
17 on the page that allows you to see other people's
18 voter information.

19 Do you see that?

20 A. Yes.

21 Q. And then Mr. Barnes responds -- Michael
22 Barnes responds the same day.

23 Do you see that?

24 A. Where is Barnes? Oh, yeah, here.

25 Q. And then if you keep scrolling up

1 you'll see on -- let's see, the middle of the
2 third page there's an e-mail from Dave Hamilton
3 on August 12th, 2020 at 6:03 p.m.

4 Do you see that?

5 A. Yes.

6 Q. And that one is to you, right?

7 A. Yep.

8 Q. What do you recall about this situation
9 and the vulnerability alleged in the -- the
10 initial e-mail?

11 A. So it looks like this is a -- if I
12 remember right, this was a county website, not
13 the Secretary of State website, had a similar
14 issue with their system where people could go in
15 and pull up prior polling locations. In other
16 words, by taking the web address and incrementing
17 the number backwards, you could pull up prior
18 documents. So, again, it was not a breach, but
19 bad coding practice that needed to be fixed. And
20 you could go back in time and see the last X
21 number of documents that people had pulled up.
22 But you wouldn't be able to change anything. It
23 just was bad practice.

24 So that's why he said it was similar to
25 what we addressed with PCC on our website. So

1 that would be the -- the problem we had with the
2 MVP page where you could increment the number and
3 see other peoples' documents that they had
4 pulled, you know, up until a point that the
5 server clears cache.

6 Q. And was this -- sorry. Was this
7 remediated?

8 A. As far as I know, it was remediated
9 fairly quickly because we explained to them how
10 to fix it.

11 Q. And what's the basis for your
12 understanding that it was remediated?

13 A. It seems to me I had a conversation
14 with Dave afterwards that he had worked with them
15 to -- to understand -- you know, explain to them
16 what it was to fix. I think they actually pulled
17 the page down until they could fix it.

18 (Exhibit 16: E-mail string with the top
19 from Chris Harvey dated 12/30/2020 marked
20 for identification, as of this date.)

21 Q. Okay. All right. Grab Exhibit 16,
22 please.

23 A. Chris Harvey, voter registration
24 certificate.

25 Q. Yes.

1 So this is an e-mail you can see that
2 Chris Harvey received on December 30th, 2020.

3 Do you see that from Ryan Germany?

4 A. Yes, yes.

5 Q. And if you come down the beginning of
6 the thread it begins with an e-mail that Dave
7 Hamilton sent on December 24, 2020.

8 Do you see that?

9 A. Yes.

10 Q. And he sends that to you and Mr.
11 Germany at the Secretary's office, right?

12 A. Okay.

13 Q. And the subject line is 2020 rule
14 590-8-3 attestation and assessment.

15 Do you see that?

16 A. Yes.

17 Q. And this concerns the assessment
18 attestation or certification that the Secretary's
19 office has to put out each year, it's a security
20 risk assessment that the Secretary has to attest
21 to each year, right?

22 A. Yes.

23 Q. And so Mr. Hamilton looks like was
24 handling the attestation in December of 2020.

25 Do you recall that?

1 A. I know it gets done every year, so --
2 and it needs to be the done the first -- by the
3 end of the year or at least before -- you know,
4 early on. I think the target is by the end of
5 December.

6 Q. Okay. So do you see here --

7 A. I vaguely remember this.

8 Q. Okay. You see Mr. Hamilton writes
9 Civix just got me the last two artifacts for
10 this; do you see that?

11 A. Yes.

12 Q. What is Civix?

13 A. Civix is PCC. PCC changed their name
14 to Civix.

15 Q. Okay. And he goes on, They apparently
16 have never completed a security risk assessment.
17 Do you see that?

18 A. Yes.

19 Q. And do you have any reason to believe
20 that Mr. Hamilton was wrong about whether Civix
21 or PCC had ever completed a security risk
22 assessment?

23 MR. DENTON: Objection.

24 A. I can't speak to that.

25 Q. Okay.

1 A. I know he -- Dave was a hard-core
2 security person and he didn't like -- he was
3 basically -- was very much this is how he felt
4 things should be done. People doing something a
5 different way rubbed him. So this doesn't
6 surprise me.

7 Q. And Hamilton was the chief information
8 security officer while he was at the Secretary's
9 office, right?

10 A. Yes.

11 Q. Okay.

12 A. He did a good job.

13 Q. If you come to the second paragraph, do
14 you see he writes, Hope this suffices. I did my
15 level best to meet all of these items. Not sure
16 how James ever signed this with a straight face.

17 Do you see that?

18 A. Yep.

19 Q. And by James he's referring to James
20 Oliver, the former security manager, right?

21 A. Yes.

22 Q. And did you share Mr. Hamilton's
23 concern about how James Oliver was able to sign
24 this attestation in prior years?

25 A. As I said --

1 MR. DENTON: Objection.

2 A. -- Dave was a -- I'll say a
3 perfectionist. He was very judgmental of other
4 people. And if they didn't do things his way, he
5 wasn't satisfied. There are lots of people in
6 the securities world. Dave was a very hard-core
7 and that he had his vision of how things should
8 be done. Not that his was the only way to do
9 something, but he had his way and he spoke his
10 mind. Here he is speaking his mind. Whether or
11 not James actually met the level of the law, I
12 felt he did.

13 Now, did Dave have a harder view on
14 things and drive the organization better? Yeah,
15 he did. That's why he essentially replaced
16 James. But James did what he was supposed to do.
17 He worked within the legal law of what
18 requirements were. Dave was unhappy with Civix
19 because he -- his view on security was one thing
20 and they had a different. Security is a broad
21 topic. Dave was very opinionated and he
22 basically would voice his opinion all the time.
23 So you're reading it.

24 Q. And the concern that Dave Hamilton
25 expresses in this e-mail thread is that the --

1 the Secretary of State is actually not in
2 compliance with the rule at this time because he
3 can't find the evidence, what he calls artifacts,
4 of that compliance, right?

5 MR. DENTON: Objection.

6 A. Yeah. He doesn't say here what the
7 artifacts are. I know he and I have talked about
8 this on multiple occasions. As I said, he was a
9 perfectionist. The attestation applies only,
10 only to the voting -- voter registration system,
11 the election system. Dave felt it should apply
12 to all things that the Secretary of State
13 managed. But the attestation specifically only
14 applied to election. So Dave was always on a --
15 on a course to say we should have things like
16 artifacts that cover everything, whether it's the
17 corporate registration system, whether it is the
18 security system, professional licensing system.
19 He felt all of them should fall under the same
20 level of security that elections did. But the
21 attestation clearly does not include anything but
22 elections. And that was always a rub to Dave.

23 Does that answer your question?

24 Q. I think so. I was going to grab
25 another exhibit for you.

1 A. Oh, all right I didn't -- one of those
2 pregnant pause moments --

3 Q. Yes. Sorry.

4 (Exhibit 17: E-mail string with the top
5 from Dave Hamilton dated 12/21/2020 marked
6 for identification, as of this date.)

7 Q. All right. Grab Exhibit 17.

8 A. This looks like it's the same topic.

9 Q. Yes, yes, a little bit earlier. So I
10 wanted to -- a little more context.

11 So if you go to the top, you'll see
12 this is an e-mail that Dave Hamilton sent you on
13 December 21, 2020 regarding the rule 590 -- or
14 the 590 rule attestation, right?

15 A. Okay.

16 Q. If you come down in the earliest e-mail
17 of the thread is an e-mail that Mr. Hamilton
18 sends to you December 19, 2020 and he copies
19 itsecurity@sos.ga.gov.

20 Do you see that?

21 A. Yes.

22 Q. What is the IT security e-mail there?
23 Is that some sort of like team or group
24 distribution list?

25 A. It's just an e-mail box that if we

1 have, like, vendors sending reports, like
2 Cybraics is one of our monitoring systems. It
3 monitors network traffic between nodes inside the
4 network. It sends out a regular e-mail of alerts
5 of activity and stuff like that. Rather than
6 having it go to a specific security person, it
7 goes to a security -- IT security mailbox that
8 all of the security people see.

9 Q. Okay. Do you know whether that e-mail
10 in box was searched for relevant e-mails for this
11 case?

12 A. If we do a search on 365, it's
13 included, which would be the answer is yes, it
14 was included.

15 Q. Meaning if they did a search on 39- --
16 365 that it encompassed that e-mail advice?

17 A. It should, yes.

18 MR. DENTON: Objection.

19 Q. Okay. All right. So Mr. Hamilton
20 writes here regarding this rule attestation in
21 the first sentence and started after the comma,
22 he writes, I really don't understand how my
23 predecessor was ever able to attest to meeting
24 the set of regulations. I handled this just like
25 an assessment. If we can't come up with an

1 artifact that proves something is real, it
2 doesn't exist.

3 Do you see that?

4 A. Yep.

5 Q. And do you agree with Mr. Hamilton, the
6 former CISO's position, that for the attestation
7 provided by this rule, that if you cannot come up
8 with an artifact that proves that something is
9 real, it doesn't exist?

10 A. This is the same response I gave the
11 last one, which is he had a view of an
12 attestation that was broader than the rule
13 actually is written for. And he was trying to
14 position that we should cover all systems under
15 that attestation, thus find artifacts that
16 basically mark our -- you know, that we meet the
17 590 rule across every system. Well, there are
18 things that are in 590 that the other systems
19 don't necessarily do. I don't have that list.
20 But I know that that's part -- that was his big
21 rub. And so that's -- he's -- this was probably
22 his -- one of his early sort of discoveries as
23 he's trying to go through that list and find
24 those artifacts. And he's looking for them for
25 systems outside of what 590 truly covers, which

1 is the election system, and he can't find them.
2 Because they don't exist because not everything
3 that's in 590 applies to all systems for
4 Secretary of State. He wanted them to, but they
5 didn't. So he was frustrated.

6 Q. So if you come up to the e-mail that he
7 sent you on December 21 and come down towards the
8 bottom of the page, you see that paragraph that
9 begins on our part, we did everything?

10 A. Yes.

11 Q. And then the third line at the end he
12 writes, My plan was to produce an amendment
13 shortly after the first of the year. Once E-Net
14 lands and I can verify the risk gaps are
15 minimized.

16 Do you see that?

17 A. No. I've lost you. I'm down on the
18 first -- bottom of the first page.

19 Q. Yeah, the paragraph that reads, on our
20 part.

21 A. Oh, yeah. Okay. We did everything we
22 could to meet these rules.

23 Q. Come to the end of the third line, the
24 sentence begins my plan.

25 A. The one that says, My plan has to

1 produce an amendment?

2 Q. Yes.

3 Do you know what was meant by once
4 E-Net lands?

5 A. No.

6 Q. Was there any change contemplated with
7 E-Net at this time that you recall?

8 A. No. I don't know of any.

9 Q. Okay. And then he then goes on -- he
10 goes on to the third paragraph -- the next
11 paragraph -- two paragraphs after that. You see
12 where it reads, the largest impact? And he
13 writes, The largest impact can be made by getting
14 Civix to produce their part of this. We can go
15 from 66 percent up to over 80 percent quickly.

16 Do you see that?

17 A. Yep.

18 Q. And what Mr. Hamilton found at this
19 time, was it looking only at PCC or what he
20 refers to here as Civix, the state was only --
21 only at 66 percent in compliance with what's
22 required under this rule, right?

23 A. I don't know the context.

24 Q. What do you mean you don't know the
25 context? This is an e-mail that he sent to you?

1 A. Yes. But he's saying we can go from 66
2 up to over 80 quickly. I don't know whether he's
3 talking about the context of Civix in like --
4 like we talked earlier, fixing their code so that
5 they can't do sequel injection and things like
6 that so we don't have to use external tools to
7 remediate, that could very well be where he is.
8 Because that was also a big thing is he wanted
9 them to fix their code so it was a true fix, not
10 a remediation using a different solution. That
11 could very well be where he's talking. And if
12 you notice this date timeline is all around that
13 same time frame.

14 Q. Okay. But do you understand that the
15 concern he was expressing was that with respect
16 to what PCC was handling, the state was only in
17 compliance with 66 percent of the requirements
18 under the rule based on --

19 MR. DENTON: Objection.

20 Q. -- research he had done?

21 A. I see that. As I said, Civix code did
22 not meet some of the requirements that we had to
23 have from security inspection. So we had to put
24 things in front of it to reach the level of
25 security we needed. He was a truest. He wanted

1 the code to do it on its own.

2 So we've already talked about this
3 topic of Civix couldn't fix their code to do what
4 it is because it would break it. And they would
5 have to do a major rewrite to do what really
6 needed to do to fix the sequel injection, the
7 cross-side scripting, those kind of things.

8 Q. Okay.

9 A. They didn't like the fact that we had
10 to use other tools like Cloudflare to fix
11 problems to meet our attestation levels. He
12 wanted to see them -- like he said, we could
13 quickly get there if Civix would just fix this.
14 We knew that. But we couldn't -- we -- get them
15 to fix it.

16 Q. All right.

17 A. It was a point of frustration for him.

18 Q. The Secretary's office has announced
19 that they're actually moving away from E-Net,
20 right?

21 A. Yes.

22 Q. And why is that?

23 A. It's an old system, to start with.
24 Civix has changed vendors -- or has been
25 purchased I think at least twice, maybe three

1 times in the last four years, four or five years.

2 Q. When was the decision made to move away
3 from E-Net?

4 A. Last year.

5 Q. Who made that decision?

6 A. Front office.

7 Q. And by front office who do you mean?

8 A. Secretary.

9 Q. Oh, Secretary Raffensperger?

10 A. Yes. Those kind of decisions, it comes
11 down to him to make the call. We present
12 proposals and it's up to him to say yay, nay.

13 Q. What --

14 A. It's a big decision.

15 Q. Sorry.

16 A. Yeah, that was a big, big decision.

17 Q. What were those specific reasons that
18 he decided to move -- to replace E-Net?

19 A. One was the age, one was the ability
20 for us to get, like this, certain fixes put in
21 place that we wanted to see. Some of it was
22 security related, some was just functionality
23 related. The application was built I think like
24 in 2012 when we first purchased it. And the --
25 but the actual application was probably built a

1 year or two before that. So the core code was
2 ten years old. Getting very old. Technology has
3 changed. So it was time to look at another
4 solution. We were in the process of also looking
5 at some of our other systems and we decided to do
6 basically an overall refit of everything.

7 Q. What's the new solution that you're
8 bringing in in place of E-Net?

9 A. I think they've announced -- already
10 announced that it's Salesforce based.

11 Q. And will that be a cloud solution
12 hosted by Salesforce?

13 A. Yes.

14 Q. Okay. What's the process for migrating
15 data from E-Net to Salesforce; do you know?

16 A. It hasn't been done yet. We're in the
17 process of trying to come up with a migration
18 plan.

19 (Exhibit 18: 2020 Security of the voter
20 registration system artifacts and
21 attestation pursuant to Rule 590-8-3-.01
22 December 18, 2020 marked for
23 identification, as of this date.)

24 Q. All right. Grab Exhibit 18, please.

25 A. 2020 security of voter registration

1 system, artifacts and attestation.

2 Q. Yeah, so we're still on the same
3 subject of the same time frame of the e-mails we
4 were looking at between you and Mr. Hamilton
5 about this rule attestation.

6 Do you see that?

7 A. Yes.

8 Q. And this is dated December 18, 2020.
9 Do you see that on the front page?

10 A. Yes, I've got it.

11 Q. And if you come down to the bottom of
12 the cover page, do you see David Hamilton's
13 signature is there next to CISO?

14 A. You're saying all the way to the
15 bottom?

16 Q. If you just go to the bottom of the
17 first page. Not the end of the whole document.

18 A. Oh, bottom of the first page. Sorry, I
19 went to the bottom of the document.

20 Q. Yeah, sorry.

21 Bottom of the first page, you'll see
22 his signature there.

23 A. Yeah.

24 Q. So okay. I'm sorry, you said yes?

25 A. Yes, I did.

1 Q. And then have you seen this before?

2 Is this -- do you recall him
3 circulating this to you?

4 A. He probably copied me on it. I don't
5 know that I read it completely. I can tell you
6 at 40 some pages I doubt I read the whole thing.

7 Q. Okay.

8 A. We probably talked through it.

9 Q. If you come to page 6 of the PDF,
10 you'll see it says Executive Summary.

11 Do you have that?

12 A. I'm looking for -- what year -- you
13 don't know what page that is, do you?

14 Q. Page 6. If you look in the bottom
15 right corner, it's page 6. And at the top it
16 says, Executive Summary.

17 A. Got it. Yep.

18 Q. And here in the second paragraph it
19 states, Currently our agency does not, not is in
20 all caps, meet the requirements of the rule. Out
21 of the 38 requirements, we only meet 66 percent.
22 Most short falls are Civix related. If we accept
23 their items, we are at 81 percent, which is
24 better.

25 Do you see that?

1 A. Yes.

2 Q. And if you come down below that, do you
3 see the dashboard?

4 A. Yes.

5 Q. And under -- it's got a -- a subsection
6 of the rule, a description and then status,
7 whether it's met, fully met, partially met not
8 met or an exception.

9 Do you see that?

10 A. Yes.

11 Q. And am I reading this right that what
12 -- what's indicated in the dashboard below, that
13 indicates what Mr. Hamilton concluded about
14 whether some -- each particular subsection of the
15 rule is met at this time?

16 A. Yes. That's his perspective.

17 Q. Okay. All right. We've been going a
18 while. Why don't we take another short break,
19 Mr. Beaver, and then we'll -- we'll get you out
20 of. Sorry, you need to leave by 4:15; is that
21 right?

22 A. Yes.

23 Q. Okay. All right. Let's take a short
24 break.

25 THE VIDEOGRAPHER: The time is 2:24.

1 whole technology team.

2 Q. All right. Can you come back, if you
3 would, please, to Exhibit 19, which was the cover
4 e-mail for the remediation task list.

5 A. Got it.

6 Q. And so in Mr. Hamilton's e-mail to you
7 he writes, How much do we want to share of this?
8 Normally how we prioritize and what we are
9 working on is not ever meant for public eyes.
10 And then he goes on to say, This level of detail
11 I don't think we should give anyone outside the
12 agency because it can be used to pinpoint where
13 our holes are and give a road map to bad actors.

14 Do you see that?

15 A. Yep.

16 Q. Did you share his concern that if you
17 were going to make public the attachment that it
18 could be used to pinpoint where holes were in the
19 Secretary's network and give a road map to bad
20 actors?

21 A. I think anytime you reveal any security
22 information about an organization, you give a
23 road map to bad actors. That is -- that is like
24 the number one thing that bad actors look for is
25 any public information about how a system's

1 designed, known information about it. That's why
2 bad actors typically scan sites all the time
3 looking for holes. So anytime you give them
4 something, that's not good. You're just
5 basically making it even more difficult on
6 yourself to protect your system.

7 Q. If you can pull up Exhibit 20 again.

8 A. Yes.

9 Q. Are there any specific risks in here
10 that you can identify as an example where it --
11 you would be concerned about making them public
12 because of the road map concern?

13 A. I don't know that I can answer that. I
14 -- any risk -- this is what you hear in the paper
15 all the time that, you know, Adobe has no risk.
16 Well, more than likely nobody knows about it but
17 maybe a researcher someplace. But as soon as you
18 open it up, now people can say oh, let me go look
19 over there. I mean, the Internet is a wide
20 field. As soon as you start to point to well,
21 here is a potential area, it let's people focus
22 on that and you would become more exposed.

23 That doesn't mean that the risk it --
24 probability of somebody actually penetrating it
25 is very high at all. Because somebody still has

1 A. So the typical configuration of the
2 office is you have a desk on one side, you turn
3 one way and you're working on your PC for daily
4 e-mail and stuff and it's tied to the Internet.
5 And you turn around and you face the opposite
6 direction and you're working on PC that's on the
7 air gap network.

8 Q. Got it.

9 Okay. And so I may have said this
10 before. How many people have those PCs in their
11 offices? Just approximately.

12 A. Oh, five, maybe eight. It's depending
13 on -- I think at the beginning when we had a big
14 push we had as many as eight. But I think
15 they're down to about five now.

16 Q. Okay. And then if you come to where --
17 see where it says supports SQL Express and Win
18 10, do you see that, just where we were?

19 A. Yes.

20 Q. And then below that it reads, Windows
21 10 running XP guest to access old system.

22 Do you see that?

23 A. Yes.

24 Q. Do you know what that refers to?

25 A. So we were still -- remember we were

1 running in parallel in a different environment,
2 the old GEMS system. Because we hadn't
3 completely switched over. So they were -- as
4 part of the project they had to make sure that
5 they had the machines that could run the old
6 system, they had machines that could run the new
7 system. The old system had to run XP because the
8 GEMS application run -- ran with XP.

9 Q. All right.

10 A. Two totally different environments.

11 Q. And just so I understand, when you say
12 two totally different environments, the Dominion
13 EMS server you said was locked in the cage
14 somewhere. Was the old GEMS system, whatever
15 servers it was still running on, was that locked
16 in a different cage somewhere?

17 A. It was in a different rack. A
18 different rack. You know what a rack is?

19 Q. Yes, yes, yes. So it's all in the same
20 locked cage?

21 A. Locked area.

22 Q. But it's on a different server rack?

23 A. Yes.

24 Q. Got it.

25 And you're saying there were no -- no

REPORTER'S CERTIFICATE

I, V. Dario Stanziola, a Certified Court Reporter in the State of Georgia, duly commissioned and authorized to administer oaths and to take and certify depositions, do hereby certify that on Wednesday, February 2, 2022, Sanford Merritt Beaver, being by me personally duly sworn to tell the truth, thereupon testified as above set forth as found in the preceding pages, this examination being recorded stenographically by me verbatim and then reduced to typewritten form by me, that the foregoing is a true and correct transcript of said proceedings to the best of my ability and understanding; that I am not related to any of the parties to this action; that I am not interested in the outcome of this case; that I am not of counsel nor in the employ of any of the parties to this action.

IN WITNESS WHEREOF, I have hereto set my hand, this the 8th day of February 2022.



V. DARIO STANZIOLA, CCR (GA) (NJ), RPR, CRR
Certification Number: 4531-3928-0743-6288